

SECURITY OF CDF AIRCRAFT AND AVIATION FACILITIES (8300)

(No. 3 November 2002)

The purpose of these procedures is to provide guidance and direction to CDF managers and operators regarding the security of the department's aviation facilities and aircraft. Aircraft security is especially important whether these aircraft are at an operational or base location.

Department aircraft must be protected against:

- Non-authorized uses of aircraft and equipment
- Sabotage
- Vandalism
- Accidental damage
- Theft

Aviation Facilities: Permanent and field operational sites listed below must be secured at all times:

- Helitack Bases
- Air Attack Bases
- Aviation Maintenance Facility
- Incident helibases

Security Plan

Each facility/base/incident shall develop a security plan specific to its location but in compliance with Level 1 requirements. This plan shall also identify a person responsible for the development, implementation and oversight of the plan and shall be designated as the aviation facility/base security point of contact. Each facility/base will have a security plan in place and reviewed by the Unit Chief, Region Chief, and Aviation Management Unit prior to the beginning of each fire season. Base and facility management shall meet with local and CDF law enforcement to discuss the implementation of this plan.

Responsibilities

Statewide: The Deputy Director for Fire Protection, upon consultation with appropriate advisors, shall be the statewide authority to designate the level of security that is applicable to any given facility/base and for what duration. The Deputy may specify additional security measures, as he/she feels appropriate. The Aviation Management Unit shall appoint an aviation security officer who is responsible for assisting individual facilities/bases/incidents in matters related to security and shall also be responsible to annually review the security plan at each Helitack and Air Attack base as well as the Aviation Maintenance Facility located in Sacramento.

Facility/Base: The Chief of Aviation Management, Unit Chiefs, and Chief Officers responsible for the operation of the Helitack and/or Air Attack bases are responsible to: appoint a security point of contact, develop specific security plans, and may, as the situation warrants, escalate the level of security for their facilities/bases. Any escalation at the local level shall be immediately conveyed through the command and control system to the Deputy Director for Fire Protection.

Incident: The Air Operations Branch Director for a specific incident shall be responsible to insure that appropriate security measures are in place at incident field sites that support helicopter or other aviation assets while assigned to the incident. The AOBBD shall have a security plan in place and available for review prior to commencing air operations.

National Homeland Security Advisory System

The Homeland Security Advisory System has been developed to identify the risk of a terrorist attack on the United States. Risk includes both the probability of an attack occurring and its potential gravity. The following National Threat Conditions each represent an increasing risk of terrorist attacks. Beneath each Threat Condition are some suggested Protective Measures.

The Threat Conditions and Associated Protection Measures are:

1. **Low Condition (Green)**. This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures they develop and implement:
 - Refining and exercising as appropriate preplanned Protective Measures;
 - Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and
 - Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.
2. **Guarded Condition (Blue)**. This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

- Checking communications with designated emergency response or command locations;
 - Reviewing and updating emergency response procedures; and
 - Providing the public with any information that would strengthen its ability to act appropriately.
3. **Elevated Condition (Yellow).** An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the Protective Measures that they will develop and implement:
- Increasing surveillance of critical locations;
 - Coordinating emergency plans as appropriate with nearby jurisdictions;
 - Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and
 - Implementing, as appropriate, contingency and emergency response plans.
4. **High Condition (Orange).** A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
- Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;
 - Taking additional precautions at public events and possibly considering alternative venues or even cancellation;
 - Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and
 - Restricting threatened facility access to essential personnel only.
5. **Severe Condition (Red).** A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

- Increasing or redirecting personnel to address critical emergency needs;
- Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources;
- Monitoring, redirecting, or constraining transportation systems; and
- Closing public and government facilities.

The U.S. Attorney General assigns threat conditions. They can be nationwide or set for a particular geographic area. The assignment of a Threat Condition shall prompt the implementation of an appropriate set of protective measures by federal agencies. Protective measures are the specific steps an organization shall take to reduce its vulnerability or increase its ability to respond during a period of heightened alert. The authority to craft and implement protective measures rests with the Federal departments and agencies. Federal department and agency heads shall submit an annual written report to the President, through the Assistant to the President for Homeland Security, describing the steps they have taken to develop and implement appropriate protective measures for each Threat Condition.

Because the aircraft used by CDF are military-owned aircraft, the CDF has developed Security Levels as protective measures to insure that CDF aircraft are not used in or harmed by terrorist activities.

Security Levels

Three levels of security have been designated as a means of tempering the degree of the CDF security response to the level of threat identified. As the threat increases the intensity of security procedures and precautions are escalated.

It is intended that permanent facilities operate in a Level 1 environment at all times.

Application

Level 1 is applied statewide and continuous. Levels 2 and 3 can be applied to specific areas being threatened and for a specific duration based upon the level and type of threat.

LEVEL 1

Definition: Daily, routine security at Helitack, Helibase and Air Attack bases.

- Aircraft Security: All aircraft will be locked at night or when not on standby for operational purposes. Aircraft fuel caps will be locked and disconnect helicopter batteries and lock battery compartment.
- Retardant Storage and Mixing Facilities: Air Attack bases shall take the appropriate measures to secure access to retardant supplies and mixing facilities. Locks shall be installed on mixing and storage tanks and access to dry retardant supplies shall be restricted and limited to authorized personnel.
- Facility/Base Security: Nighttime lighting will be utilized if available, base will conduct a security check each morning and evening utilizing security checklist. A single point of entry to the facility will be used when available.
- Personnel Security: Unescorted individuals need to be challenged and all visitors must sign-in and have ID verified
- Reporting Requirements: Employees will report all suspicious incidents or contacts to immediate supervisor who will, in turn, immediately report the incident upward through the command and control system.

LEVEL 2

Definition: Suspected possible security issue or heightened state of security as directed by department. This level would usually be established during a National "High" (Orange) Security Condition.

- Aircraft Security: Aircraft that cannot be secured in a hanger will be moved to a secure location designated by the Aviation Management Unit. Aircraft that cannot be moved or hangered for operational reasons or hangered will have a security guard assigned to the aircraft at night. Base personnel will ensure that the assigned security company/guards have the ECC after hours telephone number so they may notify CDF of any incidents.
- Facility/Base Security: Security guards will be posted during non-operation hours. Public tours will be suspended.
- Personnel Security: Base will be restricted to assigned personnel and necessary visitors (deliveries, management, maintenance personnel) only.
- Operate as directed by federal and state authorities.
- Reporting Requirements: Helitack and Air Attack bases will report security to ECC each morning and evening. Helibase will report security status to incident command each morning and evening. Base and Unit management will meet and coordinate with local law enforcement, CDF and other state law enforcement personnel on security issues.

LEVEL 3

Definition: Known security issue or a Governor-declared State of Emergency or State of War Emergency that creates security issues. This can be specific to a given location. This level would usually be established during a National “Severe” (Red) Security Condition.

- Aircraft Security: Move fixed-wing aircraft that are not in highly secured airport areas or helicopters to previously identified high-security bases as designated by the Aviation Management Unit (special fire suppression circumstances may dictate strategic placement of aircraft).
- Facility/Base Security: 24-hour armed guard stationed at facilities, access to facility is strictly controlled at entry points, i.e. roads, doors, gates, suspend deliveries. Ensure assigned armed guards have communication with ECC.
- Personnel Security: Base will be restricted to assigned personnel and necessary visitors (deliveries, management, maintenance personnel) who have been issued written permission to enter the facility.
- Operate as directed by federal and state authorities.
- Reporting Requirements: same as level 2

Special Concerns:

Helitack bases and Air Attack bases located at uncontrolled airports are especially vulnerable. Assigned staff should make every effort to develop a security plan that is both reasonable and effective. The inclusion of local, state, federal and department law enforcement agencies and personnel in the development and implementation of the security plan is essential.

[\(see Table of Contents\)](#)